

***Vanu, Inc.
Porter Square Galleria
One Porter Sq. #18
Cambridge MA 02140***

**ANDREW BEARD
CHIEF OPERATING OFFICER
617-864-1711 x201
ABEARD@VANU.COM**

August 1, 2003

Mr. Ed Thomas, Chief
Office of Engineering and Technology
Federal Communications Commission
445 12th Street SW
Washington DC 20554

Re: Forthcoming Notice of Inquiry on Cognitive Radios

Dear Mr. Thomas:

Following discussions with Michael Marcus and others in your office about the Commission's plan to issue a Notice of Inquiry on cognitive radios, Vanu, Inc. (Vanu) offers the observations below.

Vanu is a developer of software for software defined radio systems, and expects to participate in the market for cognitive radios.

Vanu is concerned specifically with Section 2.932(e) of the Commission's Rules, which provides:

Manufacturers must take steps to ensure that only software that has been approved with a software defined radio can be loaded into such a radio. The software must not allow the user to operate the transmitter with frequencies, output power, modulation types or other parameters outside of those that were approved. Manufacturers may use authentication codes or any other means to meet these requirements, and must describe the methods in their application for equipment authorization.¹

¹ 47 C.F.R. Sec. 2.932(e).

In adopting this provision, the Commission signaled its intent to revisit the security issue at a later date, possibly to specify more detailed security requirements.² We understand these matters may become an element of the forthcoming proceeding on cognitive radios. In that context, we ask the Commission to take account of the following.

1. Reasonable Balance

Section 2.932(e) is intended to ensure that manufacturers take reasonable steps to prevent hackers or viruses from causing radios to operate out of compliance. But we ask the Commission to note that (1) no system can be absolutely immune to a sufficiently sophisticated, subsidized, and determined intruder; and (2) increased security necessarily entails more sophisticated hardware and software -- which increases end-user costs, which in turn discourages adoption of software-defined/cognitive radios, and ultimately results in less efficient use of spectrum. The Commission should not require levels of security whose cost forecloses widespread adoption of the technology.

2. Safe Harbor

The Commission's Rules should establish a "safe harbor" with respect to future Commission action as to manufacturers whose security design practices were prudent at the time of manufacture. An encryption scheme considered safe today may be broken tomorrow; or an operating system acquired from a reputable third party may later be discovered to have a hidden flaw. The manufacturer should not be held responsible for such events.

3. Physical Security

Sometimes a well-made padlock is the best security of all. Rules on security for software-defined or cognitive radios should not require further measures for devices that are physically secured and accessible to only trusted staff. For example, a cellular telephone base station locked inside an electronics hut and connected only to the provider's private network is not accessible to hackers or viruses, and so authentication codes or similar mechanisms should not be required.

* * * *

² *Software Defined Radios*, 16 FCC Rcd 17373 at para. 32 (2001).

Mr. Ed Thomas
August 1, 2003
Page 3

I hope the above suggestions are helpful to the Commission. If you have any questions, please do not hesitate to contact me at the telephone number or email address above.

Respectfully submitted,

Andrew Beard
Chief Operating Officer
Vanu, Inc.

cc: Chairman Michael Powell
Commissioner Kathleen Q. Abernathy
Commissioner Michael J. Copps
Commissioner Kevin J. Martin
Commissioner Jonathan S. Adelstein
Michael J. Marcus, Associate Chief (Technology), OET
Julius P. Knapp, Deputy Chief, OET
Bruce A. Franca, Deputy Chief, OET
James D. Schlichting, Deputy Chief, OET
Alan J. Scrimme, Chief, Policy and Rules Division
Karen E. Rackley, Chief, Technical Rules Branch